

## Definitional Changes to HIPAA

HIPAA SECTION	CHANGE
160.103	Expands the definition of business associate to expressly include Patient Safety Organizations, Health Information Organizations, E-Prescribing Gateways, protected health information data transmission service providers with routine access to protected health information and vendors of personal health records with access to protected health information that offer access to individuals on behalf of covered entities.
160.103	A subcontractor that creates, receives, maintains or transmits protected health information on behalf of a business associate, including with respect to personal health record functions, is a HIPAA business associate and thus, is subject to the HIPAA business associate provisions
160.103	Revises the definitions of “electronic media,” “Protected Health Information,” “State” to update, clarify and conform to changes in HIPAA. Changes to HIPAA Security Rule

## Changes to HIPAA Security Rule

HIPAA SECTION	CHANGE
164.104(b)	Makes clear that, where provided, the standards, requirements, and implementation specifications of the HIPAA Privacy, Security, and Breach Notification Rules apply to business associates.
164.105(a)(2)(iii)(C)	Requires that the health care component of a hybrid entity include all business associate functions within the entity.
164.105(a)(2)(iii)(C)	With respect to a hybrid entity, the covered entity itself, and not merely the health care

	component, remains responsible for complying with business associate arrangements and other organizational requirements.
164.314(a)	Extends direct liability for compliance with the Security Rule to business associates.
164.308(b)(1) 164.308(b)(2)	Clarifies that covered entities are not required to obtain satisfactory assurances in the form of a contract or other arrangement with a business associate that is a subcontractor; rather, it is the business associate that must obtain the required satisfactory assurances from the subcontractor to protect the security of electronic protected health information.
164.314	Requires business associate agreements between business associates and subcontractors to conform to the requirements of the Security Rule.
164.314(a)(2)(i)	Contacts between a business associate and a business associate subcontractor must require compliance with the Security Rule, ensure the security of electronic protected health information and require reporting to the covered entity breaches of unsecured protected health information.

## Changes to HIPAA Privacy Rule

HIPAA SECTION	CHANGE
164.500	Clarifies that, where provided, the standards, requirements, and implementation specifications of the Privacy Rule apply to business associates.
164.502(a)(3), 164.502(a)(4)	Extends direct liability for compliance with the Privacy Rule to business associates under the Privacy Rule for impermissible uses and disclosures and for the additional HITECH requirements in Subtitle D that are made applicable to covered entities.

164.502(b)	A business associate is directly liable for failing to make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
164.502(e)(1)(ii)	Business associates are directly liable for failing to enter into business associate agreements with subcontractors that create or receive protected health information on their behalf.
164.532(d), 164.532(e)	Allows covered entities (and business associates and business associate subcontractors) to continue to operate under certain existing contracts for up to one year beyond the compliance date of the revisions to the Rules.
164.502(a)(5)(ii)	Requires a covered entity to obtain an authorization for any disclosure of protected health information in exchange for direct or indirect remuneration from or on behalf of the recipient of the information and to require that the authorization state that the disclosure will result in remuneration to the covered entity.
164.502(a)(5)(ii)(B)	<p>Exceptions to the sale of protected health information include:</p> <ul style="list-style-type: none"> <li>▪ A grant or funding from a government agency to conduct a program even if, as a condition of receiving the funding, the covered entity is required to report protected health information to the agency for program oversight or other purposes.</li> <li>▪ Grants, or contracts or other arrangements to a covered entity to perform programs or activities, such as a research study, because any provision of protected health information to the payer is a byproduct of the service being provided.</li> <li>▪ The exchange of protected health information through a health information exchange (HIE) that is paid for through</li> </ul>

	<p>fees assessed on HIE participants.</p> <ul style="list-style-type: none"> <li>▪ Exchanges for remuneration for public health activities pursuant to §§ 164.512(b) or 164.514(e).</li> <li>▪ Disclosures for research purposes to the extent that the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes.</li> <li>▪ For disclosures for the transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity.</li> <li>▪ For disclosures that are otherwise required by law to ensure a covered entity can continue to meet its legal obligations without imposing an authorization requirement.</li> <li>▪ Disclosures to the individual to provide the individual with access to protected health information or an accounting of disclosures, where the fees charged for doing so are in accord with the Privacy Rule.</li> <li>▪ For treatment and payment disclosures.</li> <li>▪ For remuneration paid by a covered entity to a business associate for activities performed on behalf of a covered entity.</li> <li>▪ For remuneration to a covered entity in the form of a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for any disclosure otherwise permitted by the Privacy Rule.</li> </ul>
164.508(a)(3)	<p>For marketing communications that involve financial remuneration, the covered entity must obtain a valid authorization from the individual before using or disclosing protected health information for such purposes, and such authorization must disclose the fact that the covered entity is receiving financial remuneration from a third party.</p>

164.508(a)(5)	Where the individual signs an authorization to receive such communications, the covered entity may use and disclose the individual's protected health information for the purposes of making such communications unless or until the individual revokes the authorization.
164.508(a)(3)(i), 164.501	<p>Exceptions to the marketing individual authorization requirement include:</p> <ul style="list-style-type: none"> <li>▪ For a face-to-face treatment or health care operations communication by a covered entity to an individual for which a covered entity receives financial remuneration from a third party or a promotional gift of nominal value provided by the covered entity.</li> <li>▪ Communications regarding refill reminders or otherwise about a drug or biologic that is currently being prescribed for the individual, provided any financial remuneration received by the covered entity for making the communication is reasonably related to the covered entity's cost of making the communication.</li> </ul>
164.502(a)(3), 164.502(a)(4)	Allows business associates to use or disclose protected health information only as permitted or required by their business associate contracts or other arrangements or as required by law.
164.502(b)	Modifies the minimum necessary standard to require that when business associates use, disclose, or request protected health information from another covered entity, they limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
164.502(e)	Allows a business associate to disclose protected health information to a business associate that is a subcontractor, and allows the subcontractor to create or receive protected health information on its behalf,

	if the business associate obtains satisfactory assurances that the subcontractor will appropriately safeguard the information.
164.504(e)	Aligns the requirements for business associate agreements with the requirements for covered entities under the HITECH Act.
164.508(b)(3)	Allows a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities, except for research that involves the use or disclosure of psychotherapy notes.
164.508(c)(1)(iv)	Reinterprets the “purpose” provision for research authorizations to no longer require that an authorization for the use or disclosure of protected health information for research purposes be study specific if it adequately describes the purposes such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research.
160.103, 164.502(f)	Enables access to decedent health information by family members or others of persons who have been deceased for more than 50 years.
164.510(b)	Permits covered entities to disclose a decedent’s information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

164.512(b)(1)	Permits covered entities to disclose proof of immunization to schools where State or other law requires the school to have such information prior to admitting the student. While written authorization will no longer be required to permit this disclosure, covered entities will still be required to obtain agreement, which may be oral, from a parent, guardian or other person acting in loco parentis for the individual, or from the individual himself or herself, if the individual is an adult or emancipated minor. Also requires that covered entities document the agreement obtained under this provision.
164.514(f)	Requires that a covered entity provide, with each fundraising communication using or disclosing protected health information to target the fundraising communication, a clear and conspicuous opportunity for the individual to elect not to receive further fundraising communications that does not cause the individual to incur an undue burden or more than nominal cost.
164.514(f)	Requires that the notice of privacy practices inform individuals that a covered entity may contact them to raise funds for the covered entity and an individual has a right to opt out of receiving such communications.
164.514(f)	Prohibits a covered entity from sending fundraising communications to an individual who has elected not to receive such communications, but opt outs may apply to specific fundraising campaigns rather than all future fundraising campaigns.
164.514(f)	Prohibits a covered entity from conditioning treatment or payment on an individual's choice with respect to receiving fundraising communications.

164.514(f)	Allows covered entities to use and disclose department of service information, treating physician information, and outcome information for fundraising purposes.
164.520(b)(1)(ii)(E)	Requires covered entities to include in their notice of privacy a statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of protected health information for marketing purposes, and disclosures that constitute a sale of protected health information require authorization, as well as a statement that other uses and disclosures not described in the notice will be made only with written authorization from the individual.
164.520(b)(1)(v)(a)	Requires covered entities to include in their notice of privacy practice a statement of the right of affected individuals to be notified following a breach of unsecured protected health information.
164.522(a)(1)(vi)(B)	Requires a covered entity to agree to a request to restrict disclosure of protected health information to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full. This is an exception to the general rule that a covered entity is not required to agree to a request for restrictions on the use or disclosure of protected health information allowed under the Privacy Rule.
164.524(c)(2)(ii)	Requires that if an individual requests an electronic copy of protected health information that is maintained electronically in one or more designated record sets, a covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable

	electronic form and format as agreed to by the covered entity and the individual
164.524 (c)(3)	Provides that, if requested by an individual, a covered entity must transmit the copy of protected health information directly to another person designated by the individual. The request must be made in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the protected health information
164.524(c)(4)(i)	Identify separately the labor for copying protected health information, whether in paper or electronic form, as one factor that may be included in a reasonable cost-based fee for a copy of protected health information.
164.524(c)(4)(ii)	Provides separately for the cost of supplies for creating the paper copy or electronic media (i.e., physical media such as a compact disc (CD) or universal serial bus (USB) flash drive), if the individual requests that the electronic copy be provided on portable media.
164.524(b)(2)(iii)	Modifies the timeliness requirements for right to access and to obtain a copy of protected health information from 60 days to 30 days with a 30-day extension when necessary.

### **Changes to HIPAA Privacy Rule under GINA**

HIPAA SECTION	CHANGE
164.502(a)(5)	Prohibits health plans from using or disclosing protected health information that is genetic information for underwriting purposes.
164.502(a)(1)(iv)	An individual authorization could not be used to permit a use or disclosure of

	genetic information for underwriting purposes.
164.502(a)(1)(iv), 160.103	Adopts several definitional modifications to the HIPAA Privacy Rule, including: <ul style="list-style-type: none"> <li>▪ Revises the definition of “health information” to make clear that the term includes “genetic information;”</li> <li>▪ Adds definitions for the GINA-related terms of “family member,” “genetic information,” “genetic services,” “genetic test,” and “manifestation or manifested;”</li> <li>▪ Makes technical corrections to the definition of “health plan.”</li> </ul>
164.501	Adds a definition of “underwriting purposes” and makes conforming changes to the definitions of “payment” and “health care operations.”
160.101, 164.504(f)(1)(ii), 164.506(a), 164.514(g)	Adopts several conforming amendments to existing HIPAA Privacy Rule sections to avoid confusion and to make clear that a health plan that receives protected health information that is genetic information is not permitted to use or disclose such information for underwriting purposes.
164.520(b)(1)(iii)(D)	Requires health plans that use or disclose protected health information for underwriting purposes to include a statement in their notice of privacy practices that they are prohibited from using or disclosing protected health information that is genetic information about an individual for such purposes.

### **Changes to HIPAA Enforcement Rule and Civil Money Penalty Structure**

HIPAA SECTION	CHANGE
160.306(c)(1)	Makes clear that the Secretary will investigate any complaint filed under the Enforcement Rule when a preliminary

	review of the facts indicates a possible violation due to willful neglect.
160.306(c)(2)	Gives the Secretary continued discretion with respect to investigating any other complaints.
160.308(a)	Provides that the Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provision when a preliminary review of the facts indicates a possible violation due to willful neglect.
160.308(b)	Gives the Secretary continued discretion to conduct compliance reviews in circumstances not indicating willful neglect.
160.310(c)(3)	Allows the Secretary to disclose protected health information if permitted under the Privacy Act to allow the Secretary to coordinate with other law enforcement agencies.
160.312(a)	Allows, rather than requires, the Secretary to attempt to resolve investigations or compliance reviews indicating noncompliance by informal means.
160.401	Modifies the definition of “reasonable cause” to clarify the mens rea associated with the reasonable cause category of violations and to clarify the full scope of violations that will come within the category.
160.404	Establishes four categories of violations that reflect increasing levels of culpability and four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation. ▪ If culpability is “did not know” then

	<p>penalty of \$100-\$50,000 for each violation, with \$1,500,000 maximum penalty for all such violations of an identical provision in a calendar year.</p> <ul style="list-style-type: none"> <li>▪ If culpability is “reasonable cause” then penalty of \$1,000-\$50,000 for each violation, with \$1,500,000 maximum penalty for all such violations of an identical provision in a calendar year.</li> <li>▪ If culpability is “willful neglect” with correction, then penalty of \$10,000-\$50,000 for each violation, with \$1,500,000 maximum penalty for all such violations of an identical provision in a calendar year.</li> <li>▪ If culpability is “willful neglect” without correction then penalty of \$50,000 for each violation, with \$1,500,000 maximum penalty for all such violations of an identical provision in a calendar year.</li> </ul>
N/A	Removes the previous affirmative defense to the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation.
160.410	Provides a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.
160.504	Allows an entity that believes that a civil money penalty has been imposed unfairly, to appeal the imposition of a civil money penalty in a hearing before an administrative law judge.
160.402(c)	Makes covered entities and business associates liable for the acts of their business associate agents regardless of whether the covered entity has a compliant business associate agreement in place.
160.410	Provides that the Secretary’s authority to impose a civil money penalty will be

	barred only to the extent a covered entity or business associate can demonstrate that a criminal penalty has been imposed.
160.412	Provides the Secretary with the authority to waive a civil money penalty, in whole or in part, for violations described in § 160.410(b)(2) or § 160.410(c) that are not corrected within the period specified.
160.420(a)(4)	Requires the Secretary identify in a notice of proposed determination the applicable violation category upon which the proposed penalty amount is based.
160.408(a)	Requires the Secretary to consider five general factors, each with more specific factors that may be considered, in determining a civil money penalty. <ol style="list-style-type: none"> <li>1. The nature and extent of the violation. <ol style="list-style-type: none"> <li>a. Time period during which the violation(s) occurred.</li> <li>b. The number of individuals affected.</li> </ol> </li> <li>2. The nature and extent of the harm resulting from the violation. <ol style="list-style-type: none"> <li>a. Reputational harm.</li> </ol> </li> <li>3. The history of prior compliance with the administrative simplification provision, including violations by the covered entity or business associate. <ol style="list-style-type: none"> <li>a. Indication of non-compliance</li> </ol> </li> <li>4. The financial condition of the covered entity or business associate.</li> <li>5. Such other matters as justice may require.</li> </ol>

### **Changes to HIPAA Enforcement Rule and Civil Money Penalty Structure**

HIPAA SECTION	CHANGE
160.402(2)	Clarified that breach notification is necessary in all situations except those in which the covered entity or business associate demonstrates, through risk assessment, that there is a low probability

	the PHI has been compromised.
160.402(2)	<p>A risk assessment must consider at least the following factors:</p> <ul style="list-style-type: none"><li>▪ The nature and extent of the PHI involved, including the types of identifiers and the likelihood or re-identification.</li><li>▪ The unauthorized person who used the PHI or to whom the disclosure was made.</li><li>▪ Whether the PHI was actually acquired or viewed/</li><li>▪ The extent to which the risk to the PHI has been mitigated.</li></ul>